

Hon. Sheldon H. Weisberg  
Chief Judge, Arizona Court of Appeals, Division One  
1501 W. Washington  
Phoenix, AZ 85007  
(602) 542-1434

R-03-0012

**IN THE SUPREME COURT OF THE STATE OF ARIZONA**

In the Matter of:	)	
Rule 123, Arizona Rules of the Supreme Court	)	Supreme Court
Rules of Civil Procedure and Rules of	)	R. No. 2003-_____
Criminal Procedure	)	
_____	)	

**PETITION TO AMEND RULE 123 OF THE ARIZONA SUPREME COURT RULES**

Pursuant to Rule 28 of the Rules of the Supreme Court, Hon. Sheldon H. Weisberg, Chairman of the Ad Hoc Committee to Study Public Access to Electronic Court Records, petitions the Supreme Court to amend Rule 123 of the Rules of the Supreme Court as specified in the amendment attached as Exhibit A, and to adopt the proposed new rules for the mandatory use of a confidential sensitive data form, as specified in Exhibit B.

**GROUND FOR APPROVAL OF PETITION**

In August 2000, Administrative Order No. 2000-54 established the *Ad Hoc* Committee to Study Public Access to Electronic Court Records and charged the committee to examine:

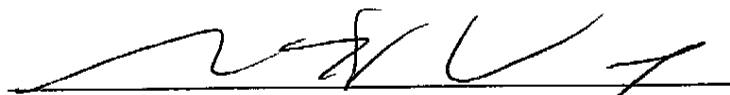
[T]he issues surrounding public access to computerized court records, including disclosure of bulk data, and develop recommendations to modify Rule 123, and to suggest additional rules governing access to information which may be contained within a computer program or other electronic media. The committee's recommendations must take into account the importance of balancing individual privacy and confidentiality with the public's interest in access to the court's case and administrative records. The committee should articulate a sound basis for any distinctions it draws between access policies relating to paper records and access policies relating to electronic records.

The Committee undertook a comprehensive review of the issues that included how well the current rule addresses hard copy and electronic public access to court records, related policy studies from other

jurisdictions, data gathering practices in Arizona courts and what types of sensitive data are routinely found in case files. The committee also heard from representatives of the trial bench, court clerks and administrators, litigators, prosecutors, law enforcement, the news media, private investigators, behavioral health specialists, domestic violence and victims' rights advocates and the Arizona Civil Liberties Union. The Committee's study is more fully reported in its October 2002 Report and Recommendations, attached hereto as Exhibit C and incorporated herein by reference. This report and the recommendations contained therein were unanimously adopted by Arizona Judicial Council on October 17, 2002. The recommendations propose a number of modifications to the way courts collect personal information from litigants, as well as recommending specific changes to Rule 123. This petition seeks to effectuate those Committee proposals that are amenable to implementation through the Rule 28 process.

For the foregoing reasons, petitioner urges the Supreme Court to amend Supreme Court Rule 123 as set forth in the attached Exhibit A and adopt the practice of requiring use of a confidential sensitive data form as proposed in Exhibit B .

Respectfully submitted, this 2nd day of May, 2003.



Hon. Sheldon H. Weisberg, Petitioner  
Chairman, *Ad Hoc* Committee to Study Public Access to  
Electronic Court Records  
Chief Judge, Arizona Court of Appeals, Division One  
1501 W. Washington  
Phoenix, AZ 85007  
(602) 542-1434

## EXHIBIT A

(Changes or additions in text are indicated by underlining and deletions from text are indicated by ~~strikcouts~~.)

### RULES OF THE SUPREME COURT OF ARIZONA

#### Rule 123. Public Access to the Judicial Records of the State of Arizona

(a) **Authority and Scope of Rule.** [no change to text]

(b) **Definitions.**

(1) through (12) [no change to text]

X (13) *Sensitive Data.* “Sensitive data” means social security number, bank account number, credit card number, other financial account number, a victim’s address and phone number, and a juvenile victim’s name.

(c) **General Provisions.** [no change to text]

(d) **Access to Case Records.**

(1) through (3) [no change to text]

X (4) *Sensitive Data Form.* The clerk shall maintain the sensitive data form as a confidential record accessible by the general public only on a showing of good cause pursuant to the process set forth in subsection (f). Good cause may include access by a media representative for purposes of researching a news story.

(e) **Access to Administrative Records.**

All administrative records are open to the public except as provided herein:

(1)-(7) [no change to text]

OK (8) *Remote Electronic Access Logs.* Records maintained by any court which show that a user of a remote electronic access system has accessed a particular court record are closed.

(8)(9) *Attorney and Judicial Work Product.* [renumbered, no change to text]

(9)(10) *Juror Records.* [renumbered, no change to text]

(10)(11) *Proprietary and Licensed Material.* [renumbered, no change to text]

(11)(12) *Copyrighted Documents and Materials*. [renumbered, no change to text]

(f) **Access to Records in Paper Medium**. [no change to text]

(g) **Access to Audiotape, Videotape, Microfilm, Computer or Electronic Based Records**.

(1) through (4) [no change to text]

(5) *Remote Electronic Access to Records and Cost; Limitations on Remote Access*.

(A) through (C) [no change to text]

OK (D) Any on-line electronic access shall be conditioned upon the user's agreement to access the information only as instructed by the court, to not attempt any unauthorized access, and to consent to monitoring by the court of all use of the system. The court will also notify users that it will not be liable for inaccurate or untimely information, or for misinterpretation or misuse of the data, and that viewers' disclosure of such information to third parties is done at their own risk. Viewers must also be instructed to rely only on the official version of the case file, available at the court house. Such agreement and notices shall be provided to the users by prominently displaying them on any court Web site offering case information ~~any manner the court deems appropriate~~. The court may deny access to users for failure to comply with such requirements.

(E) [no change to text]

OK (F) The presiding judge of each court may establish limitations on remote electronic access based on the needs of the court, limitations on technology and equipment, staff resources and funding. Court Web sites offering case information should also offer a glossary or other online resources that will facilitate viewers' understanding of the case information offered.

(G) The following records and data elements are not open to public inspection by remote electronic means:

(i) presentence reports;

(ii) criminal case exhibits, unless attached to a motion or other filing;

(iii) petitions for an order of protection or injunction against harassment;

~~(iv) parties' residential addresses;~~

(v) victims' names; and

(vi) documents, docket and calendar information on unserved orders of protection or injunctions against harassment.

OK but add addresses + delete (iv)  
The court may offer this information by remote electronic means to parties and attorneys of record in their own cases.

NO  
X +

(H) Non-confidential case documents containing unredacted sensitive data shall not be posted to a court's publicly-accessible Web site from domestic relations, juvenile, mental health or probate cases. A court may offer these records by remote electronic means to parties and attorneys of record in their own cases.

OK

(G)(I) All courts and clerks of court shall employ appropriate security measures, procedures, devices and software to protect assets and records and to prevent unauthorized access. Any court Web site offering case information shall be designed to permit users to access only one case at a time and to prevent viewing or downloading data in bulk.

(H)(J) [renumbered, no change to text]

(6) Correcting Data Errors: Administrative Review.

(A) An individual seeking to correct a data error or omission in an electronic court record shall be entitled to apply for relief with the court in which the original record was filed. If the record was filed in a superior court, the request should be made with the clerk of the superior court. If the record was filed in a justice court, the request should be made with the justice of the peace. If the record was filed in a municipal court, the request should be made to the presiding municipal court judge.

(B) If the request is denied, the individual may then apply for administrative review of that decision by the presiding superior court judge. The request for administrative review must be filed in writing with the custodian who denied the request within 10 business days of a denial. The custodian shall forward the request for review, a statement of the reason for denial and all relevant documentation to the presiding superior court judge or a designee within 3 business days of the request for review. The presiding superior court judge shall issue a decision as soon as practicable considering the nature of the request and the needs of the applicant, but not more than 10 business days from the date the written request for review was received.

(C) Any party aggrieved by the decision of the presiding judge may seek review by filing a special action in the court of appeals pursuant to the Rules of Procedure for Special Actions.

**(h) Inspection and Photocopying.** [no change to text]

X

**EXHIBIT B**

Proposed rule of procedure relating to the use of a sensitive data form

Rule \_\_\_\_\_. Sensitive Data.

**(a) Filing Sensitive Data.**

(1) Before filing any paper with the court containing sensitive data, the filing party shall omit or otherwise redact the sensitive data unless it is specifically requested by the court. If the sensitive data is specifically requested by the court, the filer shall record the requested information on a separate sensitive data form which shall be maintained by the clerk as a confidential record. Unless the court orders otherwise, any further written reference to a sensitive data element shall thereafter be made by referring to its corresponding item number on the sensitive data form or other means, rather than inserting the actual data into the document being filed with the court.

(2) Whenever new information is needed to supplement the record in a case, the parties shall file an updated sensitive data form, reflecting all previously disclosed sensitive data plus any additional sensitive data required to be filed in the case.

**(b) Sensitive Data Defined.** For purposes of this rule, “sensitive data” means social security number, bank account number, credit card number, other financial account number, juvenile victim’s name, and victim’s address or phone number.

**(c) Sensitive Data Form.** The sensitive data form shall be in substantially the following form:  
[see following page]

[Proposed Sensitive Data Form]

Name: \_\_\_\_\_

Address: \_\_\_\_\_

Phone: \_\_\_\_\_

Bar No.: \_\_\_\_\_

IN THE \_\_\_\_\_ COURT OF THE STATE OF ARIZONA  
COUNTY OF \_\_\_\_\_

_____,	)	Case No. _____
Petitioner/Plaintiff	)	
vs.	)	<b>CONFIDENTIAL</b>
_____,	)	<b>SENSITIVE DATA FORM</b>
Respondent/Defendant	)	
_____	)	

A. Social Security Numbers:

	<u>Name</u>	<u>Social Security Number</u>
1.	_____	_____
2.	_____	_____
3.	_____	_____

B. Financial Account Numbers:

	<u>Financial Institution</u>	<u>Type of Account</u>	<u>Name(s) of Account Owner</u>	<u>Account #</u>
1.	_____	_____	_____	_____
2.	_____	_____	_____	_____
3.	_____	_____	_____	_____

C. Juvenile Victim's Name/Contact Information (applicable to crime victims under age 18):

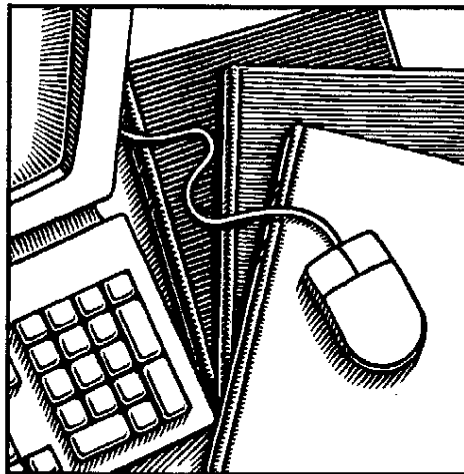
	<u>Name</u>	<u>Address</u>	<u>Phone Number</u>
1.	_____	_____	_____
2.	_____	_____	_____

D. Victim's Residential Address (the name of a crime victim who is not a juvenile is not deemed "sensitive" and therefore is not made confidential by Arizona Supreme Court Rule 123, however the victim's residential address is deemed "sensitive"):

	<u>Name</u>	<u>Address</u>
1.	_____	_____
2.	_____	_____
3.	_____	_____

**Ad Hoc Committee to Study  
Public Access to Electronic Court Records**

**Report  
and  
Recommendations**



**October 2002**



**EXHIBIT "C"**



**REPORT and RECOMMENDATIONS of the  
AD HOC COMMITTEE TO STUDY PUBLIC ACCESS  
TO ELECTRONIC COURT RECORDS  
OCTOBER 2002**

**TABLE OF CONTENTS**

Committee Members .....	ii
Introduction .....	1
1. Comment on the CCJ/COSCA Model Policy .....	2
2. Changes to the Committee's March 2001 Recommendations .....	2
Sensitive data and the sensitive data sheet .....	2
3. Restrictions on Access to Case Records for Protection Orders and Injunctions Against Harassment .....	2
Remote electronic access to case information .....	2
Electronic images of pleadings .....	3
Public access to paper records at the courthouse .....	3
Public access to the Court Protection Order Repository .....	3
4. Access to Criminal Records .....	4
Proposed pilot project .....	6
5. Case Information Offered on Court Web Sites .....	7
Web site consistency .....	7
Consideration of specific data elements .....	8
6. Summary List of Recommendations .....	9
Preamble .....	9
Sensitive data .....	9
Experimental release of criminal case files .....	10
Orders of protection/injunctions against harassment .....	11
Remote access to records in other types of cases .....	12
Web site management .....	12
Administrative appeal .....	13
Personal judicial e-mail .....	13

**Committee to Study Public Access  
to Electronic Court Records  
2002**

David Bodney, Esq.  
Steptoe & Johnson LLP  
Phoenix, AZ

Hon. B. Robert Dorfman  
Phoenix Municipal Court  
Phoenix, AZ

John Fearing  
Arizona Newspapers Association  
Phoenix, AZ

Michael Grant, Esq.  
Gallagher & Kennedy  
Phoenix, AZ

Rep. Jeffrey M. Hatch-Miller  
Arizona House of Representatives  
Phoenix, AZ

Karl Heckart, Director  
AOC/Information Technology Division  
Arizona Supreme Court  
Phoenix, AZ

Hon. M. Jean Hoag  
Maricopa County Superior Court, Southeast  
Mesa, AZ

Mary Hawkins  
Superior Court in Gila County  
Globe, AZ

Hon. Michael Lex  
Tucson Municipal Court  
Tucson, AZ

Philip MacDonnell, Esq.  
Jennings Strouss & Salmon PLC  
Phoenix, AZ

Hon. Clark Munger  
Pima County Superior Court, Division 19  
Tucson, AZ

Hon. Patricia Noland  
Pima County Superior Court Clerk  
Tucson, AZ

Pat Sallen, Esq.  
Phoenix, AZ

Harvey Shrednick  
ASU College of Business  
Tempe, AZ

Hon. Sheldon Weisberg, Chairman  
Arizona Court of Appeals, Division One  
Phoenix, AZ

David Withey, Esq.  
AOC/Legal Services  
Arizona Supreme Court  
Phoenix, AZ

**COMMITTEE STAFF:**

Jennifer Greene, Esq.  
Policy Analyst, Court Services Division  
Arizona Supreme Court AOC  
Phoenix, AZ

**Ad Hoc Committee to Study Public Access to Electronic Court Records**  
**REPORT AND RECOMMENDATIONS**  
**October 2002**

**Introduction**

This report and recommendations are provided in response to the March 6 and the July 10, 2002 letters from Chief Justice Charles E. Jones to Hon. Sheldon Weisberg, Chairman of the Committee to Study Public Access to Electronic Court Records ("the committee"). The letters are attached as Appendix A. In his two letters, the Chief Justice requested that this committee undertake the following matters:

1. Review and comment on a draft of the Conference of Chief Justices/Conference of State Court Administrators (CCJ/COSCA) model policy governing public access to court records.
2. Review other states' recent policy statements and determine whether the committee's March 2001 recommendations should be amended in light of these policy statements.
3. Recommend whether Supreme Court Rule 123 should be amended to impose restrictions on access to the records of cases in which an order of protection or injunction against harassment is sought, providing an explanation for any restrictions recommended.
4. Recommend exactly which categories of criminal case records should be available on the Internet addressing the data file (basic case demographics and docket information), documents and exhibits, including photographic evidence, in light of the policies adopted in the federal courts and in California to not publish such records for public inspection on the Internet.
5. Review the individual case information currently offered by Arizona court Web sites and draft recommendations pertaining to the need for consistency on what is made public or restricted. The recommendations are to specifically address whether the following data elements should be excluded from case information accessible online:
  - Party street address
  - Party city, state and/or zip code
  - Party birth date
  - Names of parties who are minors
  - Party social security number
  - Whether case information relating to orders of protection and injunctions against harassment should be restricted in some fashion.

The following report details the committee's efforts on each of these tasks.

### **1. Comment on the CCJ/COSCA Model Policy**

The committee's comment on the model policy is attached as Appendix B. It was provided to the model policy work group via e-mail on May 2, 2002.

### **2. Changes to the Committee's March 2001 Recommendations**

#### **Sensitive data and the sensitive data sheet**

The committee has reviewed its report of March 2001 and recommends that its initial recommendation relating to the sensitive data sheet be amended to state that the sensitive data sheet should be a confidential record, accessible by the public only on a showing of good cause pursuant to the administrative process set forth in Rule 123. This change in recommendations is based on the concern that were this one document to be publicly available, too much sensitive financial information (social security numbers, bank and credit card account numbers) could be easily culled from any case file, possibly promoting identity theft or other fraud.

The committee also identified two additional types of case information that should appear only on a sensitive data sheet: victim contact information (address/phone number) and juvenile victims' names. Victims' rights advocates have related to the committee that unregulated dissemination of this information profoundly concerns many victims. Recent changes in statutes and rules have extended special privacy considerations to this class of citizens, and so a majority of committee members felt it appropriate to recommend that this information be removed from non-confidential court documents.

Further revisions to the committee's original recommendations are specified in other parts of this report.

### **3. Restrictions on Access to Case Records for Protection Orders and Injunctions Against Harassment**

The committee heard from members of the Committee on the Impact of Domestic Violence in the Courts (CDVIC) and other interested public members and formulated the following recommendations relating to records and case information in these types of cases:

#### **Remote electronic access to case information**

No Internet access should be offered to the public on petitions for orders of protection, injunctions against work place harassment or injunctions against harassment until the order has been served on the responding party. This prohibition extends to docket-type information and calendar information.

Justification: Respondents who learn of unserved orders may dodge service. Petitioners may need time to implement a safety plan before serving a defendant.

Electronic images of pleadings

No electronic images of petitions for an order of protection, an injunction against work place harassment or an injunction against harassment should be offered to the public via the Internet.

Justification: Uncorroborated allegations of criminal conduct often appear in the petition for an order of protection or for an injunction against harassment or against work place harassment. Confidential case records and information are not available to the public in paper format, therefore, access to this information should not be offered to the general public over the Internet.

Public access to paper records at the courthouse

The current public access policy permitting traditional access *at the courthouse* to case files for orders of protection or injunctions against work place harassment or injunctions against harassment should not be diminished.

Justification: The subcommittee is unaware of any significant problems that the current policy has created for litigants or the general public.

Public access to the Court Protection Order Repository

If the general public is granted access to the Court Protection Order Repository (CPOR), the same restrictions should apply as recommended above.

Justification: The subcommittee understands the CPOR database has been created for use by courts and law enforcement primarily. The information contained in the CPOR database is a subset of the data contained in the data warehouse maintained by the Administrative Office of the Courts. It is a logistical question whether it is easier to provide public access to this database as opposed to extracting information from the data warehouse directly. The committee does not take a position on whether the public should be provided with access to the non-confidential, post-service records from this database. Regardless of the source of the information, all restricted data would need to be filtered out, blocked or otherwise redacted from the publicly-accessible version of this database.

#### **4. Access to Criminal Case Records**

The committee reviewed other states' policies concerning online access to criminal case records and docket information. Compared to the five other jurisdictions that have articulated a policy to date, the Arizona committee recommendations would permit the most wide-open access. While all jurisdictions agree that remote electronic access to basic case information such as case dockets and calendars should be available, California, Florida, Massachusetts and the federal district courts have decided against offering electronic access to images of the actual documents filed in criminal cases for the time being. Maryland has decided to make such records available but only on the court's private dial-up network, which requires registration and payment of an annual \$50 user fee. The federal district courts are currently engaged in a two-year pilot project that offers remote electronic access to criminal case records from eleven district courts. Users of the system must register for a user name and password, and their use of the records can be tracked and logged by the court. The federal courts also charge a fee of seven cents per page for use.

The committee heard from a panel of prosecutors, criminal defense attorneys, representatives of the Arizona Criminal Justice Commission and the director of a victim assistance program. Panel members uniformly urged the committee to restrict online access to criminal case records, and raised the following concerns about Internet access to litigation files for criminal and juvenile records:

- Although some victims would prefer to keep current with the progress of their cases via the Internet, others would be "panicked" by the thought of having their names, addresses and descriptions of their victimization widely available (especially true for victims of sex crimes). Indictments often contain a lot of the types of information which victims do not want published on the Internet. Victims have a constitutional right to be free of intimidation, and this level of access may facilitate harassment and intimidation of victims. These concerns extend to victims of domestic violence who may be identified on orders of protection.
- Remote electronic access to court records may pose problems for domestic violence victims who are seeking employment, because employers may not want to hire a person who has sought a protection order.
- Law enforcement investigative efforts may be impaired if witnesses are reluctant to come forward for fear that their identities will be disclosed on the Internet.
- A defendant's right to a fair trial may be jeopardized if jurors could use the Internet to research a defendant's criminal history.
- Criminals might use case information to learn the whereabouts of prosecutors they wish to target for assault.
- Courts are not compelled to post criminal records to the Internet, and the substantial difference in the level of access this offers to the general public is a new phenomenon which the committee should fully consider and understand before recommending litigation files be posted to the Internet.

- User logs need to be maintained to track who is accessing particular records; without logs there is no accountability.
- If the defendant contests the amount of restitution owed, written evidence regarding a victim's medical treatment or financial accounts is often filed with the court without being sealed.
- Criminals are using the Internet to create their own databases of personal information including images of signatures, which can be used to forge documents and apply for credit cards in other people's names (a form of identity theft).
- Free Internet access to public records impedes government agencies from recouping the cost of maintaining records.

In light of the electronic access policies recently announced by other jurisdictions, and the concerns expressed by the law enforcement, criminal defense and victims' rights communities, the committee believes it is appropriate to proceed more cautiously than originally recommended. At the same time, it is important to gather solid evidence on which to make a durable policy. The policy debate on this important issue has proceeded without the benefit of knowing exactly what consequences may flow from offering criminal case records to the general public over the Internet.

The federal trial courts are currently engaged in a pilot project offering remote electronic public access to images of documents from criminal case files by means of a subscription service. The Arizona policy could conceivably await the results of this pilot project, due in September 2003. At the same time however, far fewer people ever become involved with the federal criminal courts than is true of state courts. The results of the federal pilot may not accurately predict the experience with state court criminal files. Accordingly, the committee recommends that the Arizona judicial department conduct its own pilot project to determine the costs and benefits of offering remote electronic access to state court criminal case files. Only with the knowledge gained from such a study can an electronic access policy be forged that will stand the test of time and avoid serious unintended consequences.

The proposal accommodates many of the concerns expressed by the representatives of the Attorney General's Office, the County Attorney's Office, the Arizona Criminal Justice Commission and the crime victim community. The courts will be accountable for who is using the system and will know where users have been. By design, the program discourages the idly curious and anonymous viewers. We suspect that those willing to register and pay fees will be the same users who regularly patronize the clerk's customer service counter, namely those with a legitimate need to know.

This program offers the type of enhanced access that Rule 123 already envisions, and will give the courts an opportunity to measure whether wider remote access by the general public will be an appropriate use of technology.

Proposed Pilot Project:

Internet access to criminal case files should be offered to the public on a pilot basis for 3 years, under the following parameters:

- Users will be required to register and obtain a user name and password. Registration will be in-person or on-line; applicants must provide proof of identification. Subscribers should be required to renew their subscriptions every 3 years and notify the court of address changes.
- In applying for a user name and password, potential subscribers will be asked to sign or accept the following statement:

I understand that the password issued to me shall not be used by any other individual and that unauthorized use of my password or a breach of any security procedures related to the use of my password may be a violation of A.R.S. sections 13-2316 and 13-2316.01.

- The subscriber application form should notify potential subscribers that their use will be monitored for quality control, gathering statistics and to prevent misuse, and that their user privileges may be revoked or suspended without notice at any time, pursuant to Rule 123(g)(5)(D).
- Use of the website should be tracked by the court, so that a record will be made of the specific records accessed by a particular user.
- Subsection (e) of Rule 123 should be amended to read:

**(e)(8) Remote electronic access logs.** Records maintained in any court which link a user of a remote electronic access system to the court records viewed or downloaded are closed.

Rule 123(b)(1) defines a closed record as one that the public may not inspect, copy or otherwise access unless authorized by law.

- The following contents of criminal records will not be accessible via remote electronic access:



- Exhibits introduced at a hearing or trial, whether admitted into evidence or not. Exhibits attached to any motion or other filing will be accessible unless sealed.
  - Other documents which the committee previously recommended be kept off line including presentence reports and the sensitive data sheet.
  - Other documents excluded from public access by Rule 123.
  - Any reference to a victim's address or other contact information or a juvenile victim's name must be redacted before the record in which this information appears can be viewed by registered users.
- Users, other than parties and attorneys of record for their specific cases, will be required to pay a fee for registration and a fee for use sufficient to cover the court's cost of providing access, maintaining the registration logs and tracking use of the electronic records by the registered users.
  - A.R.S. section 12-284.02 (and its counterparts applicable to the appellate and lower jurisdiction courts (A.R.S. §§ 12-119.02 (supreme court records), 22-284 (justice court) & 22-408 (municipal court records)) should be amended to permit more flexibility in setting fees for electronic access to court records as needed.
  - The pilot program of access to criminal case documents will reveal the advantages and disadvantages of offering this type of access to the public, and a mechanism should be created to track and report these observations. The pilot project should be reviewed by the Arizona Judicial Council prior to the end of the pilot project.
  - Free public Internet access to basic case information such as dockets and calendars for criminal cases should continue.

## **5. Case Information Offered on Court Web Sites**

### **Web site consistency**

In his letter of March 6, the Chief Justice asked the committee to draft recommendations pertaining to the need for consistency on what is made public or restricted on judicial Web sites. The committee recommends that this issue be designated a new project either of this committee or a new committee. Tackling this issue will require an examination of each case type and data element in order to recommend

what information should or should not be offered over the Internet for individual cases within each case type.

The committee has reviewed the data elements and case types offered on each of the four Arizona court Web sites that provide individual case information from their case management systems, and the Supreme Court's Web page which offers select data on individual cases from approximately 100 courts contributing to the data warehouse.

The Web sites reviewed are: Pima County Consolidated Justice Courts (<http://jp.co.pima.az.us>); Maricopa Superior Court ([www.superiorcourt.maricopa.gov](http://www.superiorcourt.maricopa.gov)); Clerk of Court in Pima County ([www.cosc.co.pima.az.us](http://www.cosc.co.pima.az.us)); Court of Appeals, Division II ([www.apltwo.ct.state.az.us](http://www.apltwo.ct.state.az.us)); and Supreme Court ([www.supreme.state.az.us](http://www.supreme.state.az.us)). The committee was reluctant to mandate consistency in the information these Websites provide without more input from information technology specialists, attorneys and other interested parties who make use of this information on a regular basis. The committee is therefore recommending that this issue be pursued by a new committee or an extension of the current *ad hoc* committee's term.

#### Consideration of specific data elements

In his letter of July 10, the Chief Justice asked the committee to recommend whether the following data elements should be excluded from case information accessible online:

- Party street address
- Party city, state and/or zip code
- Party birth date
- Names of parties who are minors
- Party social security number
- Whether case information relating to orders of protection and injunctions against harassment should be restricted in some fashion.

The committee's recommendations on orders of protection and injunctions against harassment are detailed above. To reiterate, the committee is recommending that nothing be offered online in these types of cases before the order is served.

The committee also agreed that none of the following data elements should be displayed on court Web sites offering information from individual cases:

- Party social security number
- Party street address
- Names of victims

The committee recognized that some unique identifiers were helpful in distinguishing one John Smith from another, and that any combination of birth dates and/or city, state or zip code could be useful for that purpose without running the risk of facilitating identity theft. The committee saw no reason to restrict access to minor parties' names in non-confidential cases, such as traffic or criminal cases. Confidential cases such as adoption and dependency matters should not be the publicly accessible online or otherwise.

The committee agreed on one other new recommendation relating to court Web sites, and that recommendation is that the supreme court impose a reporting requirement on those courts that offer Internet access to individual case information, so that the public can learn who is using these Web sites. A standardized reporting form should be developed by the AOC for this purpose.

A complete list of the committee's recommendations follows.

## **6. Summary List of Recommendations** – combining March 2001 and October 2002 Recommendations

### **Preamble**

These recommendations are premised on the traditional and continuing availability of records, both paper and electronic, at the courthouse. Nothing in these recommendations should be taken as a proposal to limit traditional public access to records at the courthouse. These recommendations should not be taken as a mandate requiring any court to provide remote Internet access to its records.

The terms "Internet access," "remote electronic access" and "online access" are used interchangeably in these recommendations.

### **Sensitive data**

1. The courts should protect from remote electronic public disclosure the following sensitive data from case files:

- Social Security Numbers
- Credit Card Numbers
- Debit Card Numbers
- Other Financial Account Numbers
- Victim contact information (address and phone number)
- Names of juvenile victims

Rule 123(c)(3) already prohibits public access to financial account and social security numbers appearing in administrative files. Every court should review its forms and processes to ensure that this information is not being gathered unnecessarily.

2. To protect the data listed in Recommendation Number 1 above, the Supreme Court should develop a sensitive data form and require its use where applicable. The sensitive data form shall be maintained by the clerk as a confidential record accessible by the general public only on a showing of good cause pursuant to the process set forth in Rule 123. Good cause may include access by a media representative for purposes of researching a news story.

3. The Supreme Court should educate judges, attorneys and the public that case records are publicly accessible and may be available via the Internet.

*Experimental release of criminal case files*

4. Internet access to criminal case files should be offered to the public on a pilot basis for 3 years, under the following parameters:

- Users will be required to register and obtain a user name and password. Registration will be in-person or on-line; applicants must provide proof of identification. Subscribers should be required to renew their subscriptions every 3 years and notify the court of address changes.
- In applying for a user name and password, potential subscribers will be asked to sign or accept the following statement:

I understand that the password issued to me shall not be used by any other individual and that unauthorized use of my password or a breach of any security procedures related to the use of my password may be a violation of A.R.S. sections 13-2316 and 13-2316.01.

- The subscriber application form should notify potential subscribers that their use will be monitored for quality control, gathering statistics and to prevent misuse, and that their user privileges may be revoked or suspended without notice at any time, pursuant to Rule 123(g)(5)(D).
- Use of the website should be tracked by the court, so that a record will be made of the specific records accessed by a particular user.
- Subsection (e) of Rule 123 should be amended to read:

**(e)(8) *Remote electronic access logs.*** Records maintained in any court which link a user of a remote

electronic access system to the court records viewed or downloaded are closed.

- The following contents of criminal records will not be accessible via remote electronic access:
  - Exhibits introduced at a hearing or trial, whether admitted into evidence or not. Exhibits attached to any motion or other filing will be accessible unless sealed.
  - Other documents which the committee previously recommended be kept off line including presentence reports and the sensitive data sheet.
  - Other documents excluded from public access by Rule 123.
  - Any reference to a victim's address or other contact information or a juvenile victim's name must be redacted before the record in which this information appears can be viewed by registered users.
- Users, other than parties and attorneys of record for their specific cases, will be required to pay a fee for registration and a fee for use sufficient to cover the court's cost of providing access, maintaining the registration logs and tracking use of the electronic records by the registered users.
- A.R.S. section 12-284.02 (and its counterparts applicable to the appellate and lower jurisdiction courts (A.R.S. §§ 12-119.02 (supreme court records), 22-284 (justice court) & 22-408 (municipal court records)) should be amended to permit more flexibility in setting fees for electronic access to court records as needed.
- The pilot program of access to criminal case documents will reveal the advantages and disadvantages of offering this type of access to the public, and a mechanism should be created to track and report these observations. The pilot project should be reviewed by the Arizona Judicial Council prior to the end of the pilot project.
- Free public Internet access to basic case information such as dockets and calendars for criminal cases should continue.

Orders of protection/injunctions against harassment cases

5. Orders of Protection and Injunctions Against Harassment:

A. No Internet access should be offered to the public on petitions for orders of protection, injunctions against work place harassment or injunctions against harassment until the order has been served on the responding party. This prohibition extends to docket-type information and calendar information.

B. No electronic images of petitions for an order of protection, an injunction against work place harassment or an injunction against harassment should be offered to the public via the Internet.

C. The current public access policy permitting traditional access at the courthouse to case files for orders of protection, injunctions against work place harassment or injunctions against harassment should not be diminished.

D. If the general public is granted access to the Court Protection Order Repository, the same restrictions should apply as recommended in (5)(A) &(B).

Remote access to records in other types of cases

6. Non-confidential case documents in the following types of cases should not be posted to the Internet unless and until the information listed in Recommendation #1 is redacted or not available via the publicly accessible Internet version of the case file:

Domestic Relations  
Juvenile  
Mental Health  
Probate

Unlike the general public, parties and attorneys of record should be afforded electronic access to their own unexpurgated case files.

Web site management

7. In addition to the information listed in Recommendation Number 1 above, the following information should *not* appear on court Websites offering information from individual cases:

- party street addresses
- victims' names

8. Remote electronic access to case information should be afforded on a case-by-case basis only; bulk data should not be electronically accessible via the Internet. Electronic access should be limited to prevent the wholesale downloading of case files or case management databases via the Internet.

9. Rule 123 should be amended to expand the disclaimer requirement of subsection (g)(5)(D). Courts offering case information via the Internet should notify viewers not only that courts are not responsible for the accuracy, timeliness, completeness, interpretation or misuse of court records, but also that viewers' re-disclosure of such information is done at their own risk. The disclaimer should be prominently displayed and should instruct viewers to rely only on the official version of the case file, available at the court house.

10. Court Websites offering case information should also offer some type of glossary or other online resources that will facilitate viewers' understanding of the docket or case information they read.

11. The committee encourages the development of standards, guidelines and funding that allow accessing electronic information of Arizona's courts from a single point of access, without infringing on the ability of a local court to release its own electronic information.

12. Courts should make periodic public reports, no less than quarterly, detailing the public's use of case lookup web sites and the subscription criminal records pilot program. The Supreme Court should develop a standardized reporting form for courts to use in meeting this requirement.

13. Further study is warranted to determine whether certain data on individual cases should be reported consistently by any court that offers online access to individual case information.

#### Administrative appeal

14. The public should be afforded an administrative appeal process to correct data errors or omissions appearing on a court's electronic database. The process should mirror the current administrative process for appealing the denial of access to court records. Administrative review of these types of complaints would be:

a) In Superior and Justice Courts: Initial complaint lodged with clerk of court or justice of the peace; administrative review by presiding judge of superior court; any further review would be by special action to the court of appeals.

b) In Municipal Courts: Initial complaint lodged with the presiding municipal court judge; administrative review by the presiding judge of the superior court; any further review would be by special action to the court of appeals.

#### Personal judicial e-mail

15. The issue of public access to personal, non-business related e-mail warrants further study by the Commission on Technology or other appropriate committee.

C

## **APPENDIX A**





# Supreme Court

STATE OF ARIZONA

ADMINISTRATIVE OFFICE OF THE COURTS

Charles E. Jones  
Chief Justice

David K. Byers  
Administrative Director  
of the Courts

March 6, 2002

Hon. Sheldon Weisberg  
Chairman,  
Committee to Study Public Access to Electronic Court Records

Re: Request for Committee Review of Various Issues

Dear Judge Weisberg:

In light of recent policy and technology developments in Arizona and elsewhere, I request that you reconvene the Committee to Study Public Access to Electronic Court Records and prepare a report and recommendations on the following matters for the October 2002 meeting of the Arizona Judicial Council:

1. Comment on the CCJ/COSCA Model Policy and Review of Other States' Recent Policy Statements.

Please have your committee review and submit comments on the model policy drafted by the Conference of Chief Justices and the Conference of State Court Administrators which was recently released. I request that the committee review its earlier recommendations and make any changes it believes are appropriate in light of these other policy statements. The two conferences will be considering the model policy at their summer meeting in late July. Comments need to be sent by April 15, 2002. The committee developing the model policy plans to hold a national public meeting on May 17th, to receive comments.

2. Orders of Protection/Injunctions Against Harassment.

The AOC recently developed a database of protective orders known as the Court Protective Order Repository (CPOR), to assist the courts and law enforcement in sharing statewide information related to served and unserved protective orders. Without CPOR, little information is available to judges, sheriff deputies and municipal police officers concerning orders issued from other counties. The current system sometimes leaves victims of domestic violence in the precarious situation of not being able to prove the validity of a protective order when protection is most

needed. The database is also designed so that Arizona order of protection data will meet the rigorous qualifications of the National Crime Information Center for posting on their nationwide database.

The new CPOR database has raised issues about public access to protective order information in both electronic and paper files. The Committee on Domestic Violence in the Courts (CIDVC) and the Limited Jurisdiction Courts Committee has recently recommended that the Committee on Public Access to Electronic Court Records review the various perspectives on this question and recommend whether Supreme Court Rule 123 should be amended to specify that certain restrictions on access be imposed on protective orders or injunctions against harassment, and if so, why?

3. Consistency of Internet-Accessible Case Information.

I am also interested in the committee's views on the consistency of information being released by the various courts' case lookup systems. I believe we need to set consistent practices regarding what is made public or restricted. Please review these public access sites and draft any pertinent recommendations you feel are appropriate.

4. Finally, your committee recommended to the Arizona Judicial Council (AJC) that the Arizona courts first make information on criminal case files available for public access. Since that request, both the federal courts and the Judicial Council of California have adopted policies to not publish criminal case files to the internet. Contained in the criminal case "file" (either in one file or in multiple files) are three types of information: data file - such as basic case demographics and docket information; documents; and exhibits - including photographic evidence.

Please have your committee recommend exactly which categories of information you are recommending be placed on line.

Sincerely,



Chief Justice Charles E. Jones

July 10, 2002

Honorable Sheldon Weisberg  
Chairman, Committee to Study Public Access to Electronic Court Records

Re: Request for Committee Recommendation Regarding Online Case Information

Dear Judge Weisberg:

In March we asked that you reconvene this committee to address various issues that have arisen in the past year. One of the issues identified concerned Web site consistency for the case look up sites being offered by several Arizona courts. It has come to my attention that the committee plans to advise the Arizona Judicial Council in October that this issue warrants a more thorough examination than is possible in the time remaining. The Web site consistency issue may well deserve the additional attention you are contemplating, however, the courts need guidance now on whether the following data elements should be excluded from case information accessible online:

- Party street address
- Party city, state and/or zip code
- Party birth date
- Names of parties who are minors
- Party social security number

We also need the committee's recommendation on whether case information relating to orders of protection and injunctions against harassment should be restricted in some fashion. It would be most appreciated if you could include the committee's recommendations on these matters in your report to the Arizona Judicial Council in October.

Sincerely,

Charles E. Jones  
Chief Justice

## **APPENDIX B**

TO: National Center for State Courts  
FROM: Arizona Supreme Court *Ad Hoc* Committee to Study Public Access to Electronic Court Records  
DATE: May 2, 2002  
RE: Comment on the Proposed CCJ/COSCA Model Policy on Public Access to Court Records

## INTRODUCTION TO OUR COMMENT

Arizona Supreme Court Rule 123 governing public access to court records, was initially promulgated in 1997. Arizona's *Ad Hoc* Committee to Study Public Access to *Electronic* Court Records ("the committee") (emphasis added) was created in August, 2000 in large part to respond to the emergence of the Internet as a common vehicle for offering public access to public records. Remote electronic access to court records has been the committee's focus from the beginning. The committee has *not* attempted to determine the soundness of our current laws governing the public's right of access to court records in paper format. In Arizona's courts, in-person, over-the-counter access to records has always been open, and has worked well for courts and the public, and should continue to be an option available to those wishing to review case files. Accordingly, the committee is not prepared to comment on the model rule to the extent it governs public access to records *at the courthouse* except as it may impact access to electronic records, regardless of whether the records exist in paper or electronic format.

The committee has identified several features of the model policy that conflict with the letter or spirit of the committee's recommendations or Arizona Supreme Court Rule 123. The model policy also offers several innovative ideas not contained in our current rule, which the committee may recommend incorporating into Rule 123 as useful enhancements. Our comments will be limited to addressing these portions of the model policy.

### A. INNOVATIONS OFFERED BY THE MODEL RULE

The committee agrees that, where technologically feasible, enhanced electronic access for parties and counsel of record should be offered. **Section 2.00** which excludes access by parties and attorneys from the definition of general public, promotes this type of enhanced access, and this, in turn, will promote equal access to justice and represents the type of improved customer service which information technology has long promised to provide. For those jurisdictions that limit remote public access to case docket information, it makes sense to offer the parties (and possibly victims in criminal cases) access to the actual pleadings, rulings and notices normally filed in the course of litigation.

Arizona does not have a policy comparable to **section 4.10(b)** relating to redaction of records. Some type of flag needs to be visible to alert the viewer to the missing information, but it needs to be done in such a way that the reason for redacting the information is not thwarted. This subsection apparently relates to electronic records, since it is easy to see when a paper record has been redacted from the face of the document. However, an electronic record or data in an electronic record may simply disappear.

While none of Arizona's court Web sites currently use a third party vendor, a few projects are being contemplated that would share electronic court records with private vendors. Arizona's current rule does not have an equivalent of model rule **section 7.00**, and the committee finds it would be a useful addition to our statewide rule.

## **B. POTENTIAL PROBLEMS WITH THE MODEL RULE**

### **1. Failure to distinguish between the original records filed by the litigants and the court in judicial proceedings and all other court records will result in restricting access to records that should be accessible.**

The model rule invites legal challenge and legal liability claims because **section 3.10** of the model rule defines "court record" to include the records normally maintained by a clerk in a case file, a database that contains information on cases, reports generated from a database and administrative records such as personnel records that relate to the business of the court. Case files should not be subject to the **section 4.30** access restrictions that a deputy clerk would be required to know and obey before handing out files over the counter.

From a logistical standpoint, this defies the reality of life in a courthouse. It also ignores the long tradition of open case files and the substantial legal precedent regarding judicial sealing of those records. Clerks cannot be expected to make these sorts of legal distinctions concerning case files, nor should they have to. Nor for that matter, should the court be expected to look for sensitive information in case files and seal them *sua sponte*. The parties must be held responsible for anything they file, and they generally have a choice of whether to file sensitive information or whether to leave it out of their filings. To the extent they need to file sensitive information, they should bear the responsibility for seeking an order sealing the information. This places the job of deciding whether a particular record in a case file should be treated as confidential by court rule or court order, not by the clerk behind the counter.

At most, the courts may adopt rules of pleading and practice proposed by the bar that provide for exclusion or special filing of information that should not be included in an open case file. For this reason primarily Arizona's Rule 123 distinguishes between case records and administrative records. The Arizona committee has encouraged the use of forms in recognition of increased public access to court records over the Internet. The form proposed by our committee would protect sensitive information such as social security numbers, credit card and financial account numbers from Internet access by the public by requiring parties to provide this type of information only on a designated sensitive information sheet that can be easily segregated by the clerk. This practice would reduce the likelihood that sensitive data would inadvertently appear on the Internet-accessible version of a case record.

Although many of the restrictions listed in **section 4.30** bear close resemblance to Arizona Rule 123, the model rule goes too far in applying these restrictions to the contents of public case files (i.e.

pleadings, motions, minute entries, orders, exhibits). The court may reasonably be expected to withhold information considered confidential or non-public in the databases, reports and administrative records that they create. The same is not true for records maintained in case files.

The specific proscription against access to “information about pending litigation where the court is a party” appears to obstruct the governmental transparency that we strive for here in Arizona. If this provision is intended to protect attorney or judicial work product in “pending” litigation, that is already covered by **subsections 4.30 (g) and (h)**, also the first five and last four digits of the social security number are now commonly used in business transactions, so it’s hard to know whether limiting access to part of the number will accomplish the desired objective.

The Commentary to this subsection makes a number of suggestions about what categories of records or specific records states should consider making confidential *at the courthouse*. As stated in our introduction, Arizona statutes, rules and common law favor public access to public records, and the committee is not prepared to comment on in-person access to records. The committee has recommended restrictions on such sensitive data as social security numbers, financial account numbers and pre-sentence reports.

In weighing privacy versus public Internet access to criminal records, our committee has decided that at least following conviction, it is better to side with the public’s interest in access in order to make possible self-protection and safety, rather than permitting our concerns about possible misuse of such information to dictate policy in this area. At the same time, we recognized that items such as presentence reports should always be restricted from Internet access.

Civil cases appeared to offer fewer concerns about sensitive information. The committee recommended that other types of case records, to the extent they are not made confidential by statute, should also be accessible online, once the financial account and social security numbers were scrubbed from the Internet version of the file. To accommodate the clerks’ logistical concerns, the committee also proposed a “sensitive information sheet” be made part of routine case filings to facilitate the clerks’ maintenance of sensitive data apart from the rest of an Internet-accessible case file. To the extent sensitive data must be filed in a case, the parties would use the sensitive information form to provide the information to the court. Our committee is still debating whether the sensitive data sheet should be available to the public at the courthouse.

Over the last two decades, the courts in Arizona have spent millions of dollars to move to automated case processing, and the committee’s proposed policy will maximize the benefits automation offers in customer service and operational efficiencies. In the absence of a specific identification of the harms that would flow from Internet access to case records, the more prudent course of action appears to be to continue the present policy of open access to such information.

The Commentary suggests that “unsworn allegations” not be made available online, but only at the courthouse. Since “unsworn allegations” may appear in a complaint, answer, ruling, motion or exhibit, this restriction appears to be unenforceable, at least until technology has advanced much further.

## **2. Failure to distinguish between Internet access and in-person access at the courthouse.**

The model policy does not go far enough in describing what types of records or data should be accessible by remote electronic means such as the Internet. This issue is central to the work of the Arizona committee and is plaguing court policy makers around the country. Many were looking to the C.J./COCA effort to provide a national consensus on the extent to which remote electronic access is prudent and advisable. The paucity of records specified in **section 4.70** (records presumptively subject to remote electronic access by the public) speaks volumes about the difficulty of the issue. If those are the only items which the model rule work group could agree on, the commentary should spell that out. The model rule should state the important policy considerations that underlie the work group’s recommendations.

Under Arizona’s rule, the issue of whether to offer any case information online is left to the discretion of the presiding judge of the court. Arizona’s court system is not centrally funded, and vast differences exist from court to court in terms of available funding. The committee’s recommendations are founded on the assumption that no court should be required to offer case information on the Web. Some courts simply do not have the financial resources to undertake that type of customer service. To the extent that this subsection of the model rule imposes a burden on courts to offer remote access, such a policy would be unworkable in our state.

The committee has formed a subcommittee to investigate the types of data currently offered by the five courts or clerks of court in Arizona who are posting case information on the Internet. The subcommittee has been asked to identify specific data elements it believes should or should not be offered via remote access. We hope to have a recommendation on Web site consistency by October 2002.

## **3. Records that may be inspected but not copied.**

The type of access set forth in **section 4.20** is completely foreign to Arizona’s current policy. This restriction strikes us as unenforceable. If copying is not permitted, courts may expect to find customers taking extensive notes on a laptop or otherwise, in essence copying the information. This type of restriction could also create more traffic at the courthouse. Arizona does not offer “expungement” of criminal records, except to a limited class of juvenile offenders (*see* A.R.S. section 8-349, relating to destruction of juvenile court records). The committee is unaware of any Arizona statute or rule that automatically transforms court records from public to non-public after a fixed period of time. This proposed subsection is not a good fit with Arizona practices.



#### **4. Release of bulk or compiled confidential data .**

The committee does not favor a policy such as that proposed in model rule sections 4.40 and 4.50, that permits the release of confidential information in exchange for a promise to keep it confidential. Such a policy is too difficult to enforce.

The only restriction our committee proposed for bulk data is that it not be accessible via remote electronic access, i.e. Internet access should be one-case-at-a-time. The original committee that drafted our Rule 123 debated the issue of whether to accommodate scholars and other non-commercial interests by granting them enhanced access to records. The Arizona rule avoids the problems inherent in a system (like the Arizona public records law) that would require courts to determine the commercial value of information or the appropriateness of a requestor's proposed use of data. Our current rule permits access by anyone for any purpose, although commercial users are required to pay more for certain types of access. This system has worked well so far.

#### **5. Sealing and unsealing records and Internet access to records.**

The committee believes the model rule should not specify what substantive standard to judge whether a record is available to the public (section 4.60). State statutes, rules or case law often dictate such standards, and they may differ depending upon the type of record involved. Policy considerations such as those set forth in section 4.60 should only apply in the absence of statute, rule or case precedents.

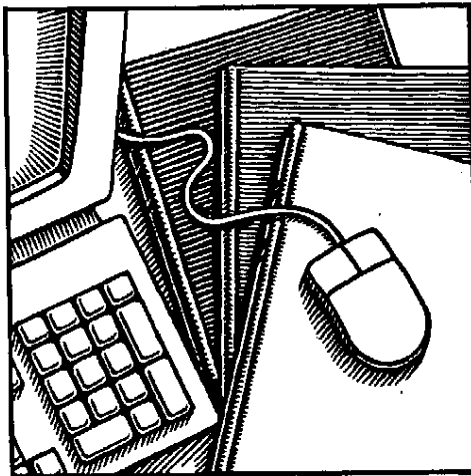
The model policy would benefit by specifying the steps necessary to open or close a record. The process could be relatively user-friendly, and probably should be geared to pro se litigants, along the lines of Arizona's administrative process for appealing the denial of a request for access to a record (see Arizona Supreme Court Rule 123(f)(5)). The committee has recommended a similar administrative process for correcting an inaccurate electronic record. All such decisions should be made by a judicial officer. A similar process could be established by which litigants could seek to prevent their records from being posted to the Internet.

#### **6. Obligation to train the public and court staff in records access policy and records correction procedures.**

The committee is concerned that the provisions of sections 8.20, 8.30 and 8.40, which impose a formal obligation on courts to train the public and court staff in public access policy, may create more problems than they solve. Obviously courts should promote the use of remote access to case information and obviously court staff should be trained in public access policy. However, the obligation may result in compliance issues and possibly even litigation by parties claiming a court has failed to fulfill its obligation. Our committee has recommended that courts endeavor to educate the public, but stopped short of requiring the courts to educate the public.

**Ad Hoc Committee to Study  
Public Access to Electronic Court Records**

**Report  
and  
Recommendations**



**October 2002**



**EXHIBIT "C"**

**REPORT and RECOMMENDATIONS of the  
AD HOC COMMITTEE TO STUDY PUBLIC ACCESS  
TO ELECTRONIC COURT RECORDS  
OCTOBER 2002**

**TABLE OF CONTENTS**

Committee Members .....	ii
Introduction .....	1
1. Comment on the CCJ/COSCA Model Policy .....	2
2. Changes to the Committee's March 2001 Recommendations .....	2
Sensitive data and the sensitive data sheet .....	2
3. Restrictions on Access to Case Records for Protection Orders and Injunctions Against Harassment .....	2
Remote electronic access to case information .....	2
Electronic images of pleadings .....	3
Public access to paper records at the courthouse .....	3
Public access to the Court Protection Order Repository .....	3
4. Access to Criminal Records .....	4
Proposed pilot project .....	6
5. Case Information Offered on Court Web Sites .....	7
Web site consistency .....	7
Consideration of specific data elements .....	8
6. Summary List of Recommendations .....	9
Preamble .....	9
Sensitive data .....	9
Experimental release of criminal case files .....	10
Orders of protection/injunctions against harassment .....	11
Remote access to records in other types of cases .....	12
Web site management .....	12
Administrative appeal .....	13
Personal judicial e-mail .....	13

**Committee to Study Public Access  
to Electronic Court Records  
2002**

David Bodney, Esq.  
Steptoe & Johnson LLP  
Phoenix, AZ

Hon. B. Robert Dorfman  
Phoenix Municipal Court  
Phoenix, AZ

John Fearing  
Arizona Newspapers Association  
Phoenix, AZ

Michael Grant, Esq.  
Gallagher & Kennedy  
Phoenix, AZ

Rep. Jeffrey M. Hatch-Miller  
Arizona House of Representatives  
Phoenix, AZ

Karl Heckart, Director  
AOC/Information Technology Division  
Arizona Supreme Court  
Phoenix, AZ

Hon. M. Jean Hoag  
Maricopa County Superior Court, Southeast  
Mesa, AZ

Mary Hawkins  
Superior Court in Gila County  
Globe, AZ

Hon. Michael Lex  
Tucson Municipal Court  
Tucson, AZ

Philip MacDonnell, Esq.  
Jennings Strouss & Salmon PLC  
Phoenix, AZ

Hon. Clark Munger  
Pima County Superior Court, Division 19  
Tucson, AZ

Hon. Patricia Noland  
Pima County Superior Court Clerk  
Tucson, AZ

Pat Sallen, Esq.  
Phoenix, AZ

Harvey Shrednick  
ASU College of Business  
Tempe, AZ

Hon. Sheldon Weisberg, Chairman  
Arizona Court of Appeals, Division One  
Phoenix, AZ

David Withey, Esq.  
AOC/Legal Services  
Arizona Supreme Court  
Phoenix, AZ

**COMMITTEE STAFF:**

Jennifer Greene, Esq.  
Policy Analyst, Court Services Division  
Arizona Supreme Court AOC  
Phoenix, AZ

**Ad Hoc Committee to Study Public Access to Electronic Court Records**  
**REPORT AND RECOMMENDATIONS**  
**October 2002**

**Introduction**

This report and recommendations are provided in response to the March 6 and the July 10, 2002 letters from Chief Justice Charles E. Jones to Hon. Sheldon Weisberg, Chairman of the Committee to Study Public Access to Electronic Court Records ("the committee"). The letters are attached as Appendix A. In his two letters, the Chief Justice requested that this committee undertake the following matters:

1. Review and comment on a draft of the Conference of Chief Justices/Conference of State Court Administrators (CCJ/COSCA) model policy governing public access to court records.
2. Review other states' recent policy statements and determine whether the committee's March 2001 recommendations should be amended in light of these policy statements.
3. Recommend whether Supreme Court Rule 123 should be amended to impose restrictions on access to the records of cases in which an order of protection or injunction against harassment is sought, providing an explanation for any restrictions recommended.
4. Recommend exactly which categories of criminal case records should be available on the Internet addressing the data file (basic case demographics and docket information), documents and exhibits, including photographic evidence, in light of the policies adopted in the federal courts and in California to not publish such records for public inspection on the Internet.
5. Review the individual case information currently offered by Arizona court Web sites and draft recommendations pertaining to the need for consistency on what is made public or restricted. The recommendations are to specifically address whether the following data elements should be excluded from case information accessible online:
  - Party street address
  - Party city, state and/or zip code
  - Party birth date
  - Names of parties who are minors
  - Party social security number
  - Whether case information relating to orders of protection and injunctions against harassment should be restricted in some fashion.

The following report details the committee's efforts on each of these tasks.

## **1. Comment on the CCJ/COSCA Model Policy**

The committee's comment on the model policy is attached as Appendix B. It was provided to the model policy work group via e-mail on May 2, 2002.

## **2. Changes to the Committee's March 2001 Recommendations**

### **Sensitive data and the sensitive data sheet**

The committee has reviewed its report of March 2001 and recommends that its initial recommendation relating to the sensitive data sheet be amended to state that the sensitive data sheet should be a confidential record, accessible by the public only on a showing of good cause pursuant to the administrative process set forth in Rule 123. This change in recommendations is based on the concern that were this one document to be publicly available, too much sensitive financial information (social security numbers, bank and credit card account numbers) could be easily culled from any case file, possibly promoting identity theft or other fraud.

The committee also identified two additional types of case information that should appear only on a sensitive data sheet: victim contact information (address/phone number) and juvenile victims' names. Victims' rights advocates have related to the committee that unregulated dissemination of this information profoundly concerns many victims. Recent changes in statutes and rules have extended special privacy considerations to this class of citizens, and so a majority of committee members felt it appropriate to recommend that this information be removed from non-confidential court documents.

Further revisions to the committee's original recommendations are specified in other parts of this report.

## **3. Restrictions on Access to Case Records for Protection Orders and Injunctions Against Harassment**

The committee heard from members of the Committee on the Impact of Domestic Violence in the Courts (CDVIC) and other interested public members and formulated the following recommendations relating to records and case information in these types of cases:

### **Remote electronic access to case information**

No Internet access should be offered to the public on petitions for orders of protection, injunctions against work place harassment or injunctions against harassment until the order has been served on the responding party. This prohibition extends to docket-type information and calendar information.

Justification: Respondents who learn of unserved orders may dodge service. Petitioners may need time to implement a safety plan before serving a defendant.

#### Electronic images of pleadings

No electronic images of petitions for an order of protection, an injunction against work place harassment or an injunction against harassment should be offered to the public via the Internet.

Justification: Uncorroborated allegations of criminal conduct often appear in the petition for an order of protection or for an injunction against harassment or against work place harassment. Confidential case records and information are not available to the public in paper format, therefore, access to this information should not be offered to the general public over the Internet.

#### Public access to paper records at the courthouse

The current public access policy permitting traditional access *at the courthouse* to case files for orders of protection or injunctions against work place harassment or injunctions against harassment should not be diminished.

Justification: The subcommittee is unaware of any significant problems that the current policy has created for litigants or the general public.

#### Public access to the Court Protection Order Repository

If the general public is granted access to the Court Protection Order Repository (CPOR), the same restrictions should apply as recommended above.

Justification: The subcommittee understands the CPOR database has been created for use by courts and law enforcement primarily. The information contained in the CPOR database is a subset of the data contained in the data warehouse maintained by the Administrative Office of the Courts. It is a logistical question whether it is easier to provide public access to this database as opposed to extracting information from the data warehouse directly. The committee does not take a position on whether the public should be provided with access to the non-confidential, post-service records from this database. Regardless of the source of the information, all restricted data would need to be filtered out, blocked or otherwise redacted from the publicly-accessible version of this database.

#### **4. Access to Criminal Case Records**

The committee reviewed other states' policies concerning online access to criminal case records and docket information. Compared to the five other jurisdictions that have articulated a policy to date, the Arizona committee recommendations would permit the most wide-open access. While all jurisdictions agree that remote electronic access to basic case information such as case dockets and calendars should be available, California, Florida, Massachusetts and the federal district courts have decided against offering electronic access to images of the actual documents filed in criminal cases for the time being. Maryland has decided to make such records available but only on the court's private dial-up network, which requires registration and payment of an annual \$50 user fee. The federal district courts are currently engaged in a two-year pilot project that offers remote electronic access to criminal case records from eleven district courts. Users of the system must register for a user name and password, and their use of the records can be tracked and logged by the court. The federal courts also charge a fee of seven cents per page for use.

The committee heard from a panel of prosecutors, criminal defense attorneys, representatives of the Arizona Criminal Justice Commission and the director of a victim assistance program. Panel members uniformly urged the committee to restrict online access to criminal case records, and raised the following concerns about Internet access to litigation files for criminal and juvenile records:

- Although some victims would prefer to keep current with the progress of their cases via the Internet, others would be "panicked" by the thought of having their names, addresses and descriptions of their victimization widely available (especially true for victims of sex crimes). Indictments often contain a lot of the types of information which victims do not want published on the Internet. Victims have a constitutional right to be free of intimidation, and this level of access may facilitate harassment and intimidation of victims. These concerns extend to victims of domestic violence who may be identified on orders of protection.
- Remote electronic access to court records may pose problems for domestic violence victims who are seeking employment, because employers may not want to hire a person who has sought a protection order.
- Law enforcement investigative efforts may be impaired if witnesses are reluctant to come forward for fear that their identities will be disclosed on the Internet.
- A defendant's right to a fair trial may be jeopardized if jurors could use the Internet to research a defendant's criminal history.
- Criminals might use case information to learn the whereabouts of prosecutors they wish to target for assault.
- Courts are not compelled to post criminal records to the Internet, and the substantial difference in the level of access this offers to the general public is a new phenomenon which the committee should fully consider and understand before recommending litigation files be posted to the Internet.



- User logs need to be maintained to track who is accessing particular records; without logs there is no accountability.
- If the defendant contests the amount of restitution owed, written evidence regarding a victim's medical treatment or financial accounts is often filed with the court without being sealed.
- Criminals are using the Internet to create their own databases of personal information including images of signatures, which can be used to forge documents and apply for credit cards in other people's names (a form of identity theft).
- Free Internet access to public records impedes government agencies from recouping the cost of maintaining records.

In light of the electronic access policies recently announced by other jurisdictions, and the concerns expressed by the law enforcement, criminal defense and victims' rights communities, the committee believes it is appropriate to proceed more cautiously than originally recommended. At the same time, it is important to gather solid evidence on which to make a durable policy. The policy debate on this important issue has proceeded without the benefit of knowing exactly what consequences may flow from offering criminal case records to the general public over the Internet.

The federal trial courts are currently engaged in a pilot project offering remote electronic public access to images of documents from criminal case files by means of a subscription service. The Arizona policy could conceivably await the results of this pilot project, due in September 2003. At the same time however, far fewer people ever become involved with the federal criminal courts than is true of state courts. The results of the federal pilot may not accurately predict the experience with state court criminal files. Accordingly, the committee recommends that the Arizona judicial department conduct its own pilot project to determine the costs and benefits of offering remote electronic access to state court criminal case files. Only with the knowledge gained from such a study can an electronic access policy be forged that will stand the test of time and avoid serious unintended consequences.

The proposal accommodates many of the concerns expressed by the representatives of the Attorney General's Office, the County Attorney's Office, the Arizona Criminal Justice Commission and the crime victim community. The courts will be accountable for who is using the system and will know where users have been. By design, the program discourages the idly curious and anonymous viewers. We suspect that those willing to register and pay fees will be the same users who regularly patronize the clerk's customer service counter, namely those with a legitimate need to know.

This program offers the type of enhanced access that Rule 123 already envisions, and will give the courts an opportunity to measure whether wider remote access by the general public will be an appropriate use of technology.

Proposed Pilot Project:

Internet access to criminal case files should be offered to the public on a pilot basis for 3 years, under the following parameters:

- Users will be required to register and obtain a user name and password. Registration will be in-person or on-line; applicants must provide proof of identification. Subscribers should be required to renew their subscriptions every 3 years and notify the court of address changes.
- In applying for a user name and password, potential subscribers will be asked to sign or accept the following statement:

I understand that the password issued to me shall not be used by any other individual and that unauthorized use of my password or a breach of any security procedures related to the use of my password may be a violation of A.R.S. sections 13-2316 and 13-2316.01.

- The subscriber application form should notify potential subscribers that their use will be monitored for quality control, gathering statistics and to prevent misuse, and that their user privileges may be revoked or suspended without notice at any time, pursuant to Rule 123(g)(5)(D).
- Use of the website should be tracked by the court, so that a record will be made of the specific records accessed by a particular user.
- Subsection (e) of Rule 123 should be amended to read:

**(e)(8) Remote electronic access logs.** Records maintained in any court which link a user of a remote electronic access system to the court records viewed or downloaded are closed.

Rule 123(b)(1) defines a closed record as one that the public may not inspect, copy or otherwise access unless authorized by law.

- The following contents of criminal records will not be accessible via remote electronic access:

- Exhibits introduced at a hearing or trial, whether admitted into evidence or not. Exhibits attached to any motion or other filing will be accessible unless sealed.
  - Other documents which the committee previously recommended be kept off line including presentence reports and the sensitive data sheet.
  - Other documents excluded from public access by Rule 123.
  - Any reference to a victim's address or other contact information or a juvenile victim's name must be redacted before the record in which this information appears can be viewed by registered users.
- Users, other than parties and attorneys of record for their specific cases, will be required to pay a fee for registration and a fee for use sufficient to cover the court's cost of providing access, maintaining the registration logs and tracking use of the electronic records by the registered users.
  - A.R.S. section 12-284.02 (and its counterparts applicable to the appellate and lower jurisdiction courts (A.R.S. §§ 12-119.02 (supreme court records), 22-284 (justice court) & 22-408 (municipal court records)) should be amended to permit more flexibility in setting fees for electronic access to court records as needed.
  - The pilot program of access to criminal case documents will reveal the advantages and disadvantages of offering this type of access to the public, and a mechanism should be created to track and report these observations. The pilot project should be reviewed by the Arizona Judicial Council prior to the end of the pilot project.
  - Free public Internet access to basic case information such as dockets and calendars for criminal cases should continue.

## **5. Case Information Offered on Court Web Sites**

### **Web site consistency**

In his letter of March 6, the Chief Justice asked the committee to draft recommendations pertaining to the need for consistency on what is made public or restricted on judicial Web sites. The committee recommends that this issue be designated a new project either of this committee or a new committee. Tackling this issue will require an examination of each case type and data element in order to recommend

what information should or should not be offered over the Internet for individual cases within each case type.

The committee has reviewed the data elements and case types offered on each of the four Arizona court Web sites that provide individual case information from their case management systems, and the Supreme Court's Web page which offers select data on individual cases from approximately 100 courts contributing to the data warehouse.

The Web sites reviewed are: Pima County Consolidated Justice Courts (<http://jp.co.pima.az.us>); Maricopa Superior Court ([www.superiorcourt.maricopa.gov](http://www.superiorcourt.maricopa.gov)); Clerk of Court in Pima County ([www.cosc.co.pima.az.us](http://www.cosc.co.pima.az.us)); Court of Appeals, Division II ([www.apltwo.ct.state.az.us](http://www.apltwo.ct.state.az.us)); and Supreme Court ([www.supreme.state.az.us](http://www.supreme.state.az.us)). The committee was reluctant to mandate consistency in the information these Websites provide without more input from information technology specialists, attorneys and other interested parties who make use of this information on a regular basis. The committee is therefore recommending that this issue be pursued by a new committee or an extension of the current *ad hoc* committee's term.

#### Consideration of specific data elements

In his letter of July 10, the Chief Justice asked the committee to recommend whether the following data elements should be excluded from case information accessible online:

- Party street address
- Party city, state and/or zip code
- Party birth date
- Names of parties who are minors
- Party social security number
- Whether case information relating to orders of protection and injunctions against harassment should be restricted in some fashion.

The committee's recommendations on orders of protection and injunctions against harassment are detailed above. To reiterate, the committee is recommending that nothing be offered online in these types of cases before the order is served.

The committee also agreed that none of the following data elements should be displayed on court Web sites offering information from individual cases:

- Party social security number
- Party street address
- Names of victims

The committee recognized that some unique identifiers were helpful in distinguishing one John Smith from another, and that any combination of birth dates and/or city, state or zip code could be useful for that purpose without running the risk of facilitating identity theft. The committee saw no reason to restrict access to minor parties' names in non-confidential cases, such as traffic or criminal cases. Confidential cases such as adoption and dependency matters should not be the publicly accessible online or otherwise.

The committee agreed on one other new recommendation relating to court Web sites, and that recommendation is that the supreme court impose a reporting requirement on those courts that offer Internet access to individual case information, so that the public can learn who is using these Web sites. A standardized reporting form should be developed by the AOC for this purpose.

A complete list of the committee's recommendations follows.

## **6. Summary List of Recommendations** – combining March 2001 and October 2002 Recommendations

### **Preamble**

These recommendations are premised on the traditional and continuing availability of records, both paper and electronic, at the courthouse. Nothing in these recommendations should be taken as a proposal to limit traditional public access to records at the courthouse. These recommendations should not be taken as a mandate requiring any court to provide remote Internet access to its records.

The terms "Internet access," "remote electronic access" and "online access" are used interchangeably in these recommendations.

### **Sensitive data**

1. The courts should protect from remote electronic public disclosure the following sensitive data from case files:

- Social Security Numbers
- Credit Card Numbers
- Debit Card Numbers
- Other Financial Account Numbers
- Victim contact information (address and phone number)
- Names of juvenile victims

Rule 123(c)(3) already prohibits public access to financial account and social security numbers appearing in administrative files. Every court should review its forms and processes to ensure that this information is not being gathered unnecessarily.

2. To protect the data listed in Recommendation Number 1 above, the Supreme Court should develop a sensitive data form and require its use where applicable. The sensitive data form shall be maintained by the clerk as a confidential record accessible by the general public only on a showing of good cause pursuant to the process set forth in Rule 123. Good cause may include access by a media representative for purposes of researching a news story.

3. The Supreme Court should educate judges, attorneys and the public that case records are publicly accessible and may be available via the Internet.

*Experimental release of criminal case files*

4. Internet access to criminal case files should be offered to the public on a pilot basis for 3 years, under the following parameters:

- Users will be required to register and obtain a user name and password. Registration will be in-person or on-line; applicants must provide proof of identification. Subscribers should be required to renew their subscriptions every 3 years and notify the court of address changes.
- In applying for a user name and password, potential subscribers will be asked to sign or accept the following statement:

I understand that the password issued to me shall not be used by any other individual and that unauthorized use of my password or a breach of any security procedures related to the use of my password may be a violation of A.R.S. sections 13-2316 and 13-2316.01.

- The subscriber application form should notify potential subscribers that their use will be monitored for quality control, gathering statistics and to prevent misuse, and that their user privileges may be revoked or suspended without notice at any time, pursuant to Rule 123(g)(5)(D).
- Use of the website should be tracked by the court, so that a record will be made of the specific records accessed by a particular user.
- Subsection (e) of Rule 123 should be amended to read:

**(e)(8) *Remote electronic access logs.*** Records maintained in any court which link a user of a remote

electronic access system to the court records viewed or downloaded are closed.

- The following contents of criminal records will not be accessible via remote electronic access:
  - Exhibits introduced at a hearing or trial, whether admitted into evidence or not. Exhibits attached to any motion or other filing will be accessible unless sealed.
  - Other documents which the committee previously recommended be kept off line including presentence reports and the sensitive data sheet.
  - Other documents excluded from public access by Rule 123.
  - Any reference to a victim's address or other contact information or a juvenile victim's name must be redacted before the record in which this information appears can be viewed by registered users.
- Users, other than parties and attorneys of record for their specific cases, will be required to pay a fee for registration and a fee for use sufficient to cover the court's cost of providing access, maintaining the registration logs and tracking use of the electronic records by the registered users.
- A.R.S. section 12-284.02 (and its counterparts applicable to the appellate and lower jurisdiction courts (A.R.S. §§ 12-119.02 (supreme court records), 22-284 (justice court) & 22-408 (municipal court records)) should be amended to permit more flexibility in setting fees for electronic access to court records as needed.
- The pilot program of access to criminal case documents will reveal the advantages and disadvantages of offering this type of access to the public, and a mechanism should be created to track and report these observations. The pilot project should be reviewed by the Arizona Judicial Council prior to the end of the pilot project.
- Free public Internet access to basic case information such as dockets and calendars for criminal cases should continue.

Orders of protection/injunctions against harassment cases

5. Orders of Protection and Injunctions Against Harassment:

A. No Internet access should be offered to the public on petitions for orders of protection, injunctions against work place harassment or injunctions against harassment until the order has been served on the responding party. This prohibition extends to docket-type information and calendar information.

B. No electronic images of petitions for an order of protection, an injunction against work place harassment or an injunction against harassment should be offered to the public via the Internet.

C. The current public access policy permitting traditional access at the courthouse to case files for orders of protection, injunctions against work place harassment or injunctions against harassment should not be diminished.

D. If the general public is granted access to the Court Protection Order Repository, the same restrictions should apply as recommended in (5)(A) &(B).

Remote access to records in other types of cases

6. Non-confidential case documents in the following types of cases should not be posted to the Internet unless and until the information listed in Recommendation #1 is redacted or not available via the publicly accessible Internet version of the case file:

Domestic Relations  
Juvenile  
Mental Health  
Probate

Unlike the general public, parties and attorneys of record should be afforded electronic access to their own unexpurgated case files.

Web site management

7. In addition to the information listed in Recommendation Number 1 above, the following information should *not* appear on court Websites offering information from individual cases:

- party street addresses
- victims' names

8. Remote electronic access to case information should be afforded on a case-by-case basis only; bulk data should not be electronically accessible via the Internet. Electronic access should be limited to prevent the wholesale downloading of case files or case management databases via the Internet.



9. Rule 123 should be amended to expand the disclaimer requirement of subsection (g)(5)(D). Courts offering case information via the Internet should notify viewers not only that courts are not responsible for the accuracy, timeliness, completeness, interpretation or misuse of court records, but also that viewers' re-disclosure of such information is done at their own risk. The disclaimer should be prominently displayed and should instruct viewers to rely only on the official version of the case file, available at the court house.
10. Court Websites offering case information should also offer some type of glossary or other online resources that will facilitate viewers' understanding of the docket or case information they read.
11. The committee encourages the development of standards, guidelines and funding that allow accessing electronic information of Arizona's courts from a single point of access, without infringing on the ability of a local court to release its own electronic information.
12. Courts should make periodic public reports, no less than quarterly, detailing the public's use of case lookup web sites and the subscription criminal records pilot program. The Supreme Court should develop a standardized reporting form for courts to use in meeting this requirement.
13. Further study is warranted to determine whether certain data on individual cases should be reported consistently by any court that offers online access to individual case information.

#### Administrative appeal

14. The public should be afforded an administrative appeal process to correct data errors or omissions appearing on a court's electronic database. The process should mirror the current administrative process for appealing the denial of access to court records. Administrative review of these types of complaints would be:

- a) In Superior and Justice Courts: Initial complaint lodged with clerk of court or justice of the peace; administrative review by presiding judge of superior court; any further review would be by special action to the court of appeals.
- b) In Municipal Courts: Initial complaint lodged with the presiding municipal court judge; administrative review by the presiding judge of the superior court; any further review would be by special action to the court of appeals.

#### Personal judicial e-mail

15. The issue of public access to personal, non-business related e-mail warrants further study by the Commission on Technology or other appropriate committee.

## **APPENDIX A**



# Supreme Court

STATE OF ARIZONA

ADMINISTRATIVE OFFICE OF THE COURTS

Charles E. Jones  
Chief Justice

David K. Byers  
Administrative Director  
of the Courts

March 6, 2002

Hon. Sheldon Weisberg  
Chairman,  
Committee to Study Public Access to Electronic Court Records

Re: Request for Committee Review of Various Issues

Dear Judge Weisberg:

In light of recent policy and technology developments in Arizona and elsewhere, I request that you reconvene the Committee to Study Public Access to Electronic Court Records and prepare a report and recommendations on the following matters for the October 2002 meeting of the Arizona Judicial Council:

1. Comment on the CCJ/COSCA Model Policy and Review of Other States' Recent Policy Statements.

Please have your committee review and submit comments on the model policy drafted by the Conference of Chief Justices and the Conference of State Court Administrators which was recently released. I request that the committee review its earlier recommendations and make any changes it believes are appropriate in light of these other policy statements. The two conferences will be considering the model policy at their summer meeting in late July. Comments need to be sent by April 15, 2002. The committee developing the model policy plans to hold a national public meeting on May 17th, to receive comments.

2. Orders of Protection/Injunctions Against Harassment.

The AOC recently developed a database of protective orders known as the Court Protective Order Repository (CPOR), to assist the courts and law enforcement in sharing statewide information related to served and unserved protective orders. Without CPOR, little information is available to judges, sheriff deputies and municipal police officers concerning orders issued from other counties. The current system sometimes leaves victims of domestic violence in the precarious situation of not being able to prove the validity of a protective order when protection is most

needed. The database is also designed so that Arizona order of protection data will meet the rigorous qualifications of the National Crime Information Center for posting on their nationwide database.

The new CPOR database has raised issues about public access to protective order information in both electronic and paper files. The Committee on Domestic Violence in the Courts (CIDVC) and the Limited Jurisdiction Courts Committee has recently recommended that the Committee on Public Access to Electronic Court Records review the various perspectives on this question and recommend whether Supreme Court Rule 123 should be amended to specify that certain restrictions on access be imposed on protective orders or injunctions against harassment, and if so, why?

3. Consistency of Internet-Accessible Case Information.

I am also interested in the committee's views on the consistency of information being released by the various courts' case lookup systems. I believe we need to set consistent practices regarding what is made public or restricted. Please review these public access sites and draft any pertinent recommendations you feel are appropriate.

4. Finally, your committee recommended to the Arizona Judicial Council (AJC) that the Arizona courts first make information on criminal case files available for public access. Since that request, both the federal courts and the Judicial Council of California have adopted policies to not publish criminal case files to the internet. Contained in the criminal case "file" (either in one file or in multiple files) are three types of information: data file - such as basic case demographics and docket information; documents; and exhibits - including photographic evidence.

Please have your committee recommend exactly which categories of information you are recommending be placed on line.

Sincerely,



Chief Justice Charles E. Jones

July 10, 2002

Honorable Sheldon Weisberg  
Chairman, Committee to Study Public Access to Electronic Court Records

Re: Request for Committee Recommendation Regarding Online Case Information

Dear Judge Weisberg:

In March we asked that you reconvene this committee to address various issues that have arisen in the past year. One of the issues identified concerned Web site consistency for the case look up sites being offered by several Arizona courts. It has come to my attention that the committee plans to advise the Arizona Judicial Council in October that this issue warrants a more thorough examination than is possible in the time remaining. The Web site consistency issue may well deserve the additional attention you are contemplating, however, the courts need guidance now on whether the following data elements should be excluded from case information accessible online:

- Party street address
- Party city, state and/or zip code
- Party birth date
- Names of parties who are minors
- Party social security number

We also need the committee's recommendation on whether case information relating to orders of protection and injunctions against harassment should be restricted in some fashion. It would be most appreciated if you could include the committee's recommendations on these matters in your report to the Arizona Judicial Council in October.

Sincerely,

Charles E. Jones  
Chief Justice

## **APPENDIX B**

TO: National Center for State Courts  
FROM: Arizona Supreme Court *Ad Hoc* Committee to Study Public Access to Electronic Court Records  
DATE: May 2, 2002  
RE: Comment on the Proposed CCI/COSCA Model Policy on Public Access to Court Records

## INTRODUCTION TO OUR COMMENT

Arizona Supreme Court Rule 123 governing public access to court records, was initially promulgated in 1997. Arizona's *Ad Hoc* Committee to Study Public Access to *Electronic* Court Records ("the committee") (emphasis added) was created in August, 2000 in large part to respond to the emergence of the Internet as a common vehicle for offering public access to public records. Remote electronic access to court records has been the committee's focus from the beginning. The committee has *not* attempted to determine the soundness of our current laws governing the public's right of access to court records in paper format. In Arizona's courts, in-person, over-the-counter access to records has always been open, and has worked well for courts and the public, and should continue to be an option available to those wishing to review case files. Accordingly, the committee is not prepared to comment on the model rule to the extent it governs public access to records *at the courthouse* except as it may impact access to electronic records, regardless of whether the records exist in paper or electronic format.

The committee has identified several features of the model policy that conflict with the letter or spirit of the committee's recommendations or Arizona Supreme Court Rule 123. The model policy also offers several innovative ideas not contained in our current rule, which the committee may recommend incorporating into Rule 123 as useful enhancements. Our comments will be limited to addressing these portions of the model policy.

### A. INNOVATIONS OFFERED BY THE MODEL RULE

The committee agrees that, where technologically feasible, enhanced electronic access for parties and counsel of record should be offered. **Section 2.00** which excludes access by parties and attorneys from the definition of general public, promotes this type of enhanced access, and this, in turn, will promote equal access to justice and represents the type of improved customer service which information technology has long promised to provide. For those jurisdictions that limit remote public access to case docket information, it makes sense to offer the parties (and possibly victims in criminal cases) access to the actual pleadings, rulings and notices normally filed in the course of litigation.

Arizona does not have a policy comparable to **section 4.10(b)** relating to redaction of records. Some type of flag needs to be visible to alert the viewer to the missing information, but it needs to be done in such a way that the reason for redacting the information is not thwarted. This subsection apparently relates to electronic records, since it is easy to see when a paper record has been redacted from the face of the document. However, an electronic record or data in an electronic record may simply disappear.

While none of Arizona's court Web sites currently use a third party vendor, a few projects are being contemplated that would share electronic court records with private vendors. Arizona's current rule does not have an equivalent of model rule section 7.00, and the committee finds it would be a useful addition to our statewide rule.

## **B. POTENTIAL PROBLEMS WITH THE MODEL RULE**

### **1. Failure to distinguish between the original records filed by the litigants and the court in judicial proceedings and all other court records will result in restricting access to records that should be accessible.**

The model rule invites legal challenge and legal liability claims because section 3.10 of the model rule defines "court record" to include the records normally maintained by a clerk in a case file, a database that contains information on cases, reports generated from a database and administrative records such as personnel records that relate to the business of the court. Case files should not be subject to the section 4.30 access restrictions that a deputy clerk would be required to know and obey before handing out files over the counter.

From a logistical standpoint, this defies the reality of life in a courthouse. It also ignores the long tradition of open case files and the substantial legal precedent regarding judicial sealing of those records. Clerks cannot be expected to make these sorts of legal distinctions concerning case files, nor should they have to. Nor for that matter, should the court be expected to look for sensitive information in case files and seal them *sua sponte*. The parties must be held responsible for anything they file, and they generally have a choice of whether to file sensitive information or whether to leave it out of their filings. To the extent they need to file sensitive information, they should bear the responsibility for seeking an order sealing the information. This places the job of deciding whether a particular record in a case file should be treated as confidential by court rule or court order, not by the clerk behind the counter.

At most, the courts may adopt rules of pleading and practice proposed by the bar that provide for exclusion or special filing of information that should not be included in an open case file. For this reason primarily Arizona's Rule 123 distinguishes between case records and administrative records. The Arizona committee has encouraged the use of forms in recognition of increased public access to court records over the Internet. The form proposed by our committee would protect sensitive information such as social security numbers, credit card and financial account numbers from Internet access by the public by requiring parties to provide this type of information only on a designated sensitive information sheet that can be easily segregated by the clerk. This practice would reduce the likelihood that sensitive data would inadvertently appear on the Internet-accessible version of a case record.

Although many of the restrictions listed in section 4.30 bear close resemblance to Arizona Rule 123, the model rule goes too far in applying these restrictions to the contents of public case files (i.e.



pleadings, motions, minute entries, orders, exhibits). The court may reasonably be expected to withhold information considered confidential or non-public in the databases, reports and administrative records that they create. The same is not true for records maintained in case files.

The specific proscription against access to "information about pending litigation where the court is a party" appears to obstruct the governmental transparency that we strive for here in Arizona. If this provision is intended to protect attorney or judicial work product in "pending" litigation, that is already covered by subsections 4.30 (g) and (h), also the first five and last four digits of the social security number are now commonly used in business transactions, so it's hard to know whether limiting access to part of the number will accomplish the desired objective.

The Commentary to this subsection makes a number of suggestions about what categories of records or specific records states should consider making confidential *at the courthouse*. As stated in our introduction, Arizona statutes, rules and common law favor public access to public records, and the committee is not prepared to comment on in-person access to records. The committee has recommended restrictions on such sensitive data as social security numbers, financial account numbers and pre-sentence reports.

In weighing privacy versus public Internet access to criminal records, our committee has decided that at least following conviction, it is better to side with the public's interest in access in order to make possible self-protection and safety, rather than permitting our concerns about possible misuse of such information to dictate policy in this area. At the same time, we recognized that items such as presentence reports should always be restricted from Internet access.

Civil cases appeared to offer fewer concerns about sensitive information. The committee recommended that other types of case records, to the extent they are not made confidential by statute, should also be accessible online, once the financial account and social security numbers were scrubbed from the Internet version of the file. To accommodate the clerks' logistical concerns, the committee also proposed a "sensitive information sheet" be made part of routine case filings to facilitate the clerks' maintenance of sensitive data apart from the rest of an Internet-accessible case file. To the extent sensitive data must be filed in a case, the parties would use the sensitive information form to provide the information to the court. Our committee is still debating whether the sensitive data sheet should be available to the public at the courthouse.

Over the last two decades, the courts in Arizona have spent millions of dollars to move to automated case processing, and the committee's proposed policy will maximize the benefits automation offers in customer service and operational efficiencies. In the absence of a specific identification of the harms that would flow from Internet access to case records, the more prudent course of action appears to be to continue the present policy of open access to such information.

The Commentary suggests that "unsworn allegations" not be made available online, but only at the courthouse. Since "unsworn allegations" may appear in a complaint, answer, ruling, motion or exhibit, this restriction appears to be unenforceable, at least until technology has advanced much further.

## **2. Failure to distinguish between Internet access and in-person access at the courthouse.**

The model policy does not go far enough in describing what types of records or data should be accessible by remote electronic means such as the Internet. This issue is central to the work of the Arizona committee and is plaguing court policy makers around the country. Many were looking to the C.J./COCA effort to provide a national consensus on the extent to which remote electronic access is prudent and advisable. The paucity of records specified in **section 4.70** (records presumptively subject to remote electronic access by the public) speaks volumes about the difficulty of the issue. If those are the only items which the model rule work group could agree on, the commentary should spell that out. The model rule should state the important policy considerations that underlie the work group's recommendations.

Under Arizona's rule, the issue of whether to offer any case information online is left to the discretion of the presiding judge of the court. Arizona's court system is not centrally funded, and vast differences exist from court to court in terms of available funding. The committee's recommendations are founded on the assumption that no court should be required to offer case information on the Web. Some courts simply do not have the financial resources to undertake that type of customer service. To the extent that this subsection of the model rule imposes a burden on courts to offer remote access, such a policy would be unworkable in our state.

The committee has formed a subcommittee to investigate the types of data currently offered by the five courts or clerks of court in Arizona who are posting case information on the Internet. The subcommittee has been asked to identify specific data elements it believes should or should not be offered via remote access. We hope to have a recommendation on Web site consistency by October 2002.

## **3. Records that may be inspected but not copied.**

The type of access set forth in **section 4.20** is completely foreign to Arizona's current policy. This restriction strikes us as unenforceable. If copying is not permitted, courts may expect to find customers taking extensive notes on a laptop or otherwise, in essence copying the information. This type of restriction could also create more traffic at the courthouse. Arizona does not offer "expungement" of criminal records, except to a limited class of juvenile offenders (see A.R.S. section 8-349, relating to destruction of juvenile court records). The committee is unaware of any Arizona statute or rule that automatically transforms court records from public to non-public after a fixed period of time. This proposed subsection is not a good fit with Arizona practices.

#### **4. Release of bulk or compiled confidential data .**

The committee does not favor a policy such as that proposed in model rule sections 4.40 and 4.50, that permits the release of confidential information in exchange for a promise to keep it confidential. Such a policy is too difficult to enforce.

The only restriction our committee proposed for bulk data is that it not be accessible via remote electronic access, i.e. Internet access should be one-case-at-a-time. The original committee that drafted our Rule 123 debated the issue of whether to accommodate scholars and other non-commercial interests by granting them enhanced access to records. The Arizona rule avoids the problems inherent in a system (like the Arizona public records law) that would require courts to determine the commercial value of information or the appropriateness of a requestor's proposed use of data. Our current rule permits access by anyone for any purpose, although commercial users are required to pay more for certain types of access. This system has worked well so far.

#### **5. Sealing and unsealing records and Internet access to records.**

The committee believes the model rule should not specify what substantive standard to judge whether a record is available to the public (section 4.60). State statutes, rules or case law often dictate such standards, and they may differ depending upon the type of record involved. Policy considerations such as those set forth in section 4.60 should only apply in the absence of statute, rule or case precedents.

The model policy would benefit by specifying the steps necessary to open or close a record. The process could be relatively user-friendly, and probably should be geared to pro se litigants, along the lines of Arizona's administrative process for appealing the denial of a request for access to a record (*see* Arizona Supreme Court Rule 123(f)(5)). The committee has recommended a similar administrative process for correcting an inaccurate electronic record. All such decisions should be made by a judicial officer. A similar process could be established by which litigants could seek to prevent their records from being posted to the Internet.

#### **6. Obligation to train the public and court staff in records access policy and records correction procedures.**

The committee is concerned that the provisions of sections 8.20, 8.30 and 8.40, which impose a formal obligation on courts to train the public and court staff in public access policy, may create more problems than they solve. Obviously courts should promote the use of remote access to case information and obviously court staff should be trained in public access policy. However, the obligation may result in compliance issues and possibly even litigation by parties claiming a court has failed to fulfill its obligation. Our committee has recommended that courts endeavor to educate the public, but stopped short of requiring the courts to educate the public.